In the Claims:

Kindly add Claim 69.

Please amend the claims as indicated.

1. (Currently Amended) A cryptosystem private key recovery device, comprising in combination:

a processor;

a nonvolatile memory space operatively coupled to said processor; and

a set of private key parameters stored in said nonvolatile memory space utilizing less storage space than the full parameter set $\{p, q, d_p, d_q, v\}$ and providing better computational efficiency than the minimal parameter set $\{p, q\}$, wherein the private key can be recovered from said set of stored private key parameters,

wherein said set of private key parameters comprises a parameter k_p, said parameter k_p is derived from k_p (p-1) mod e=1, p is a prime factor of a public modulus, and e is a given public exponent.

2. (Currently Amended) The cryptosystem private key recovery device of claim 1 further comprising said set of private key parameters defined by the parameters $\{p, q, k_p, k_q, v\}$ wherein~~ p and~~ q ~~are~~ is a given prime factor~~s~~ of a public modulus, ~~k_p and~~ k_q ~~are~~ is derived from ~~k_p (p-1) mod e=1 and~~ k_q (q-1) mod e=1, ~~e is a given public exponent~~ and v is derived from pv mod q=1.

3. (Original) The cryptosystem private key recovery device of claim 2 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]u \bmod 2^b$;

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]u \bmod 2^b$; and

wherein b is an integer such that p is less than 2^b and q is less than 2^b, and $ue \bmod 2^b = 1$.

4. (Original) The cryptosystem private key recovery device of claim 3 further comprising a private key parameter assembler for assembling the private key parameters $\{p, q, d_p, d_q, v\}$ from said stored and calculated values.

5. (Original) The cryptosystem private key recovery device of claim 2 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]/e$; and

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]/e$.

6. (Original) The cryptosystem private key recovery device of claim 5 further comprising a private key parameter assembler for assembling the private key parameters $\{p, q, d_p, d_q, v\}$ from said stored and calculated values.

7. (Currently Amended) The cryptosystem private key recovery device of claim 1 further comprising said set of private key parameters defined by the parameters $\{p, q, k_p, k_q\}$ wherein ~~p and~~ q ~~are~~ <u>is a</u> given prime factor~~s~~ of a public modulus

and~~, k_p and~~ k_q ~~are~~ is derived from ~~k_p (p-1) mod e=1 and~~ k_q (q-1) mod e=1~~, and e is a given public exponent~~.

8. (Original) The cryptosystem private key recovery device of claim 7 further comprising a v calculator in active cooperation with said processor and configured to calculate v from pv mod q=1.

9. (Original) The cryptosystem private key recovery device of claim 8 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]u \bmod 2^b$;

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]u \bmod 2^b$; and

wherein b is an integer such that p is less than 2^b and q is less than 2^b, and ue mod $2^b=1$.

10. (Original) The cryptosystem private key recovery device of claim 9 further comprising a private key parameter assembler for assembling the private key parameters $\{p, q, d_p, d_q, v\}$ from said stored and calculated values.

11. (Original) The cryptosystem private key recovery device of claim 8 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]/e$; and

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]/e$.

12. (Original) The cryptosystem private key recovery device of claim 10 further comprising a private key parameter assembler for assembling the private key parameters $\{p, q, d_p, d_q, v\}$ from said stored and calculated values.

13. (Currently Amended) The cryptosystem private key recovery device of claim 1 further comprising said set of private key parameters defined by the parameters $\{seed, k_p, k_q, v\}$ wherein ~~k_p and~~ k_q ~~are~~ is derived from ~~k_p (p-1) mod e=1 and~~ k_q (q-1) mod e=1, ~~e is a given public exponent,~~ v is derived from pv mod q=1, and seed is a value derived from a random number generator.

14. (Original) The cryptosystem private key recovery device of claim 13 further comprising:

a p calculator in active cooperation with said processor and configured to calculate p from said seed; and

a q calculator in active cooperation with said processor and configured to calculate q from said seed.

15. (Original) The cryptosystem private key recovery device of claim 14 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]u \bmod 2^b$;

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]u \bmod 2^b$; and

wherein b is an integer such that p is less than 2^b and q is less than 2^b, and $ue \bmod 2^b = 1$.

16. (Original) The cryptosystem private key recovery device of claim 15 further comprising a private key parameter assembler for assembling the private key parameters {p ,q ,d_p ,d_q , v} from said stored and calculated values.

17. (Original) The cryptosystem private key recovery device of claim 14 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]/e$; and

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]/e$.

18. (Original) The cryptosystem private key recovery device of claim 17 further comprising a private key parameter assembler for assembling the private key parameters {p ,q ,d_p ,d_q , v} from said stored and calculated values.

19. (Currently Amended) The cryptosystem private key recovery device of claim 1 further comprising said set of private key parameters defined by the parameters {seed, k_p ,k_q } wherein ~~k_p and~~ k_q ~~are~~ is derived from ~~k_p (p-1) mod e=1 and~~ k_q (q-1) mod e=1~~, e is a given public exponent,~~ and seed is a value derived from a random number generator.

20. (Original) The cryptosystem private key recovery device of claim 19 further comprising:

a p calculator in active cooperation with said processor and capable of calculating p from said seed; and

a q calculator in active cooperation with said processor and capable of calculating q from said seed.

21. (Original) The cryptosystem private key recovery device of claim 20 further comprising a v calculator in active cooperation with said processor and configured to calculate v from pv mod q=1.

22. (Original) The cryptosystem private key recovery device of claim 21 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]u \bmod 2^b$;

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]u \bmod 2^b$; and

wherein b is an integer such that p is less than 2^b and q is less than 2^b, and ue mod $2^b=1$.

23. (Original) The cryptosystem private key recovery device of claim 22 further comprising a private key parameter assembler for assembling the private key parameters $\{p, q, d_p, d_q, v\}$ from said stored and calculated values.

24. (Original) The cryptosystem private key recovery device of claim 21 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]/e$; and

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]/e$.

25. (Original) The cryptosystem private key recovery device of claim 24 further comprising a private key parameter assembler for assembling the private key parameters $\{p, q, d_p, d_q, v\}$ from said stored and calculated values.

26. (Currently Amended) ~~The~~ A cryptosystem private key recovery device ~~of claim 1 further comprising said set of private key parameters defined by the parameters {p ,q ,v} wherein p and q are given prime factors of a public modulus, and v is derived from pv mod q=1~~ comprising in combination:

a processor;

a nonvolatile memory space operatively coupled to said processor; and

a set of private key parameters stored in said nonvolatile memory space utilizing less storage space than the full parameter set $\{p, q, d_p, d_q, v\}$ and providing better computational efficiency than the minimal parameter set $\{p, q\}$,

wherein said private key recovery device is configured to recover a private key from said set of stored private key parameters utilizing equation $k_p (p-1) \bmod e=1$, wherein k_p is a private key parameter, p is a prime factor of a public modulus, and e is a given public exponent.

27. (Currently Amended) The cryptosystem private key recovery device of claim 26 further comprising~~:~~

~~a k_p calculator in active cooperation with said processor and configured to calculate k_p from k_p (p-1) mod e=1;~~

~~a k_q calculator in active cooperation with said processor and configured to calculate k_q from k_q (q-1) mod e=1; and~~

~~wherein e is a given public exponent~~ said set of private key parameters defined by the parameters {p ,q ,v} wherein q is a given prime factor of a public modulus and v is derived from pv mod q=1.

28. (Currently Amended) The cryptosystem private key recovery device of claim 27 further comprising:

~~a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]u \bmod 2^b$;~~

~~a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]u \bmod 2^b$; and~~

~~wherein b is an integer such that p is less than 2^b and q is less than 2^b, and $ue \bmod 2^b = 1$~~

a k_p calculator in active cooperation with said processor and configured to calculate k_p from k_p (p-1) mod e=1; and

a k_q calculator in active cooperation with said processor and configured to calculate k_q from k_q (q-1) mod e=1.

29. (Currently Amended) The cryptosystem private key recovery device of claim 28 further comprising: ~~a private key parameter assembler for assembling the private key parameters {p ,q ,d_p ,d_q , v} from said stored and calculated values~~

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]u \bmod 2^b$;

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]u \bmod 2^b$; and

wherein b is an integer such that p is less than 2^b and q is less than 2^b, and $ue \bmod 2^b=1$.

30. (Currently Amended) The cryptosystem private key recovery device of claim ~~27~~29 further comprising~~:~~

~~a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]/e$; and~~

~~a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]/e$~~ a private key parameter assembler for assembling the private key parameters {p ,q ,d_p ,d_q , v} from said stored and calculated values.

31. (Currently Amended) The cryptosystem private key recovery device of claim ~~30~~28 further comprising: ~~a private key parameter assembler for assembling the private key parameters {p ,q ,d_p ,d_q , v} from said stored and calculated values~~

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]/e$; and

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]/e$.

32. (Currently Amended) The cryptosystem private key recovery device of claim ~~1~~26 further comprising said set of private key parameters defined by the parameters {p ,q} wherein ~~p and~~ q ~~are~~ is a given prime factor~~s~~ of a public modulus.

33. (Currently Amended) The cryptosystem private key recovery device of claim 32 further comprising:

a k_p calculator in active cooperation with said processor and configured to calculate k_p from k_p (p-1) mod e=1; and

a k_q calculator in active cooperation with said processor and configured to calculate k_q from k_q (q-1) mod e=1~~; and~~

~~wherein e is a given public exponent.~~

34. (Original) The cryptosystem private key recovery device of claim 33 further comprising a v calculator in active cooperation with said processor and configured to calculate v from pv mod q=1.

35. (Original) The cryptosystem private key recovery device of claim 34 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]u \bmod 2^b$;

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]u \bmod 2^b$; and

wherein b is an integer such that p is less than 2^b and q is less than 2^b, and ue mod 2^b =1.

36. (Original) The cryptosystem private key recovery device of claim 35 further comprising a private key parameter assembler for assembling the private key parameters $\{p, q, d_p, d_q, v\}$ from said stored and calculated values.

37. (Original) The cryptosystem private key recovery device of claim 34 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]/e$; and

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]/e$.

38. (Original) The cryptosystem private key recovery device of claim 37 further comprising a private key parameter assembler for assembling the private key parameters $\{p, q, d_p, d_q, v\}$ from said stored and calculated values.

39. (Currently Amended) The cryptosystem private key recovery device of claim ~~1~~26 further comprising said set of private key parameters defined by the parameters {seed, v} wherein v is derived from pv mod q=1, and seed is a value derived from a random number generator.

40. (Original) The cryptosystem private key recovery device of claim 39 further comprising:

a p calculator in active cooperation with said processor and configured to calculate p from said seed; and

a q calculator in active cooperation with said processor and configured to calculate q from said seed.

41. (Currently Amended) The cryptosystem private key recovery device of claim 40 further comprising:

a k_p calculator in active cooperation with said processor and configured to calculate k_p from k_p (p-1) mod e=1; and

a k_q calculator in active cooperation with said processor and configured to calculate k_q from k_q (q-1) mod e=1~~; and~~

~~wherein e is a given public exponent~~.

42. (Original) The cryptosystem private key recovery device of claim 41 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]u \bmod 2^b$;

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]u \bmod 2^b$; and

wherein b is an integer such that p is less than 2^b and q is less than 2^b, and ue mod $2^b=1$.

43. (Original) The cryptosystem private key recovery device of claim 42 further comprising a private key parameter assembler for assembling the private key parameters {p ,q ,d_p ,d_q , v} from said stored and calculated values.

44. (Original) The cryptosystem private key recovery device of claim 41 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]/e$; and

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]/e$.

45. (Original) The cryptosystem private key recovery device of claim 44 further comprising a private key parameter assembler for assembling the private key parameters $\{p, q, d_p, d_q, v\}$ from said stored and calculated values.

46. (Currently Amended) The cryptosystem private key recovery device of claim ~~1~~26 further comprising said set of private key parameters defined by the parameters {seed~~,~~} wherein seed is a value derived from a random number generator.

47. (Original) The cryptosystem private key recovery device of claim 46 further comprising:

a p calculator in active cooperation with said processor and capable of calculating p from said seed; and

a q calculator in active cooperation with said processor and capable of calculating q from said seed.

48. (Currently Amended) The cryptosystem private key recovery device of claim 47 further comprising:

a k_p calculator in active cooperation with said processor and configured to calculate k_p from k_p (p-1) mod e=1; and

a k_q calculator in active cooperation with said processor and configured to calculate k_q from k_q (q-1) mod e=1~~; and~~

~~wherein e is a given public exponent~~.

49. (Original) The cryptosystem private key recovery device of claim 48 further comprising a v calculator in active cooperation with said processor and configured to calculate v from pv mod q=1.

50. (Original) The cryptosystem private key recovery device of claim 49 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]u \bmod 2^b$;

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]u \bmod 2^b$; and

wherein b is an integer such that p is less than 2^b and q is less than 2^b, and ue mod $2^b=1$.

51. (Original) The cryptosystem private key recovery device of claim 50 further comprising a private key parameter assembler for assembling the private key parameters $\{p, q, d_p, d_q, v\}$ from said stored and calculated values.

52. (Original) The cryptosystem private key recovery device of claim 49 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=[1+(p-1)(e-k_p)]/e$; and

a d_q calculator in active cooperation with said processor and configured to calculate d_q from $d_q=[1+(q-1)(e-k_q)]/e$.

53. (Original) The cryptosystem private key recovery device of claim 52 further comprising a private key parameter assembler for assembling the private key parameters $\{p, q, d_p, d_q, v\}$ from said stored and calculated values.

54. (Currently Amended) A cryptosystem private key recovery device, comprising in combination:

a processor;

a nonvolatile memory space operatively coupled to said processor; and

a set of private key parameters stored in said nonvolatile memory space and utilizing less storage space than the full parameter set {n, d} and providing better computational efficiency than the minimal parameter set {p, q},

<u>wherein said set of private key parameters comprises a parameter k, said parameter k is derived from k(p-1)(q-1) mod e=1, p and q are given prime factors of a public modulus, and e is a given public exponent</u>.

55. (Currently Amended) The cryptosystem private key recovery device of claim 54 further comprising said set of private key parameters defined by the parameters {p, q, k } ~~wherein p and q are given prime factors of a public modulus, k is derived from k(p-1)(q-1) mod e=1, and e is a given public exponent~~.

56. (Original) The cryptosystem private key recovery device of claim 55 further comprising a n calculator in active cooperation with said processor and configured to calculate n from n=pq.

57. (Original) The cryptosystem private key recovery device of claim 56 further comprising a d calculator in active cooperation with said processor and configured to calculate d from $d=[1+(p-1)(q-1)]t \bmod 2^{2b}$, wherein $te \bmod 2^{2b}=1$ and b is an integer such that p is less than 2^b and q is less than 2^b.

58. (Original) The cryptosystem private key recovery device of claim 57 further comprising a private key parameter assembler for assembling the private key parameters {n, d} from said stored and calculated values.

59. (Original) The cryptosystem private key recovery device of claim 56 further comprising a d calculator in active cooperation with said processor and configured to calculate d from $d=[1+(p-1)(q-1)]/e$.

60. (Original) The cryptosystem private key recovery device of claim 59 further comprising a private key parameter assembler for assembling the private key parameters {n, d} from said stored and calculated values.

61. (Original) The cryptosystem private key recovery device of claim 57 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from $d_p=d \bmod (p-1)$; and

a d_q calculator in active cooperation with said processor and configured to calculate d_q from d_q=d mod (q-1).

62. (Original) The cryptosystem private key recovery device of claim 61 further comprising a v calculator in active cooperation with said processor and configured to calculate v from pv mod q=1.

63. (Original) The cryptosystem private key recovery device of claim 62 further comprising a private key parameter assembler for assembling the private key parameters {p ,q ,d_p ,d_q , v} from said stored and calculated values.

64. (Original) The cryptosystem private key recovery device of claim 59 further comprising:

a d_p calculator in active cooperation with said processor and configured to calculate d_p from d_p=d mod (p-1); and

a d_q calculator in active cooperation with said processor and configured to calculate d_q from d_q=d mod (q-1).

65. (Original) The cryptosystem private key recovery device of claim 64 further comprising a v calculator in active cooperation with said processor and configured to calculate v from pv mod q=1.

66. (Original) The cryptosystem private key recovery device of claim 65 further comprising a private key parameter assembler for assembling the private key parameters {p ,q ,d_p ,d_q , v} from said stored and calculated values.

67. (CurrentlyAmended) A method for recovering a private key, comprising in combination:

storing private key parameters in a memory space;

utilizing less storage space for said private key parameters than the full parameter set $\{p, q, d_p, d_q, v\}$; and

providing better computational efficiency than the minimal parameter set $\{p, q\}$,

wherein said set of private key parameters comprises a parameter k_p, said parameter k_p is derived from $k_p(p-1) \bmod e=1$, p is a prime factor of a public modulus, and e is a given public exponent.

68. (CurrentlyAmended) A method for recovering a private key, comprising in combination:

storing private key parameters in a memory space;

utilizing less storage space for said private key parameters than the full parameter set $\{n, d\}$; and

providing better computational efficiency than the minimal parameter set $\{p, q\}$,

wherein said set of private key parameters comprises a parameter k, said parameter k is derived from $k(p-1)(q-1) \bmod e=1$, p and q are given prime factors of a public modulus, and e is a given public exponent.

69. (New) The cryptosystem private key recovery device of claim 31 further comprising a private key parameter assembler for assembling the private key parameters $\{p, q, d_p, d_q, v\}$ from said stored and calculated values.